University of Miami National Security & Armed Conflict Law Review

10-1-2013

# Cyber Utilities Infrastructure and Government Contracting

Corey P. Gray

## STUDENT NOTE

# Cyber Utilities Infrastructure and Government Contracting

*Corey P. Gray*[*]

Abstract

*The utilities critical infrastructure of the United States is under cyber attack and there is no plan in place to defend it. Hyper-technical phrases like "critical infrastructure" and "cyber security" often trigger muted responses, but the threat that America now faces is serious and deserves focused attention. This note takes a critical view of the deficiencies in the U.S.'s cyber security posture. It will specifically address the most pressing area, privately operated public utilities. The utilities sector provides essential services that impact the lives of every American. That sector increasingly relies on cyber systems to increase both their efficiency and profit margins. Most would agree that such reliance has improved the utilities sector. The problem, however, is that a lack of cyber security makes the sector vulnerable to potentially debilitating attacks. An attack that overrides a dam, electric grid, or nuclear facility would have a catastrophic impact on the country.*

*Congress has attempted to tackle the cyber security problem for over a decade. The obstacles posed by creating coherent cyber security are significant. At the center of the issue is a constitutional battle between civil liberties and public safety. While Congress struggles to reconcile those two competing interests, administrative agencies have the ability to implement stopgap defense measures. This note promotes using administrative agency contracting as an intermediate step towards shoring up the nation's cyber defense. There exists a cogent framework for public safety regulation of utilities through contracting. All government utility contracts have physical security and safety requirements. Through contracting, administrative agencies can require utilities companies to adhere to cyber security standards in the same way they require physical security standards. This stopgap solution would provide much needed support to a vulnerable area of national defense. Failure to act spells disaster for the U.S. in this new cyber age.*

[*] University of Miami School of Law, Class of 2014. Special thanks to Professor William Widen for supervising this writing project.

# Table of Contents

## I. INTRODUCTION

"If the enemy opens the door, you must race in."—Sun Tzu[1]

The cyber systems that control the U.S.'s critical infrastructure are under attack. To date, cyber systems have made U.S. critical infrastructure more efficient and effective. With the click of a mouse, an automated control system can regulate water flow to a dam, or electricity to a town. As a result, the U.S. has become reliant on cyber systems, particularly private-operated public utilities.[2] The increased reliance on these systems has made them vulnerable to cyber attacks.[3] Cyber aggressors target the U.S.'s utilities critical infrastructure ("utilities") to steal, deny, and destroy its capabilities. Today, sophisticated cyber aggressors launch attacks while remaining largely unidentified and undetected. The concern is that a coordinated attack could expose whole sections of the population to the risk of war-like harm without firing a single bullet.[4] This concern grows daily as the U.S.'s reliance on cyber systems outpaces its cyber security posture. The there is no national cyber defense in place to protect U.S. critical infrastructure cyber systems.[5] This unacceptable situation must be resolved.

Congress is the only governmental body that can establish a comprehensive cyber defense. Yet, it has failed to pass legislation to protect the cyber systems that control the nation's critical infrastructure. The challenges that Congress faces in creating a cyber defense network are formidable. The core issue is establishing a balance between civil liberties and public safety. Although Congress has worked for over a decade to find a solution, no legislation has materialized. Congress must work to inform the public of the threat cyber attacks pose to private businesses, as well as to the government. The private companies that make up much of the nation's critical infrastructure are a key component. These businesses have unique intergovernmental relationships. They are the U.S.'s front line of defense against cyber attacks. When they are attacked, the nation suffers. These businesses must be protected. They must also be informed of the threats cyber attacks pose to them and the nation.

Privately owned utilities are vulnerable to cyber attacks. Utility companies

---

[1] Sun Tzu, THE ART OF WAR 92 (Lionel Giles trans., Dover Publications Inc. 2002).

[2] Janet Napolitano, Sec'y, Dep't of Homeland Security, Remarks at the San Jose State Univ. Interdisciplinary Cybersecurity Program (Apr. 16, 2012), http://www.dhs.gov/news/2012/04/16/remarks-secretary-janet-napolitano-san-jose-state-university.

[3] *Id.*

[4] Tzu, *supra* note 1, at 48.

[5] David A. Fulghum, *Russia Recruited Civilians For Cyber Attacks On Georgia*, AEROSPACE DAILY & DEF. REPORT, Aug. 26, 2009, at 4.

leverage cyber control systems for the benefits, but often fail to implement basic security measures for their own protection.[6] Where increased vulnerability would generally force businesses to secure themselves, utilities remain largely unchanged. This is in large part because public-private relationship between utilities and the government makes them resistant to traditional market pressures.[7] Utility companies have traditionally had government protections that insulate them from the market.[8] Additionally, liability claims against utilities are generally subject to choice of law rules that further insulate them from liability suits.[9] As a result, utilities have little incentive to enhance their cyber security posture. These factors create fertile conditions for cyber attacks.

Utilities infrastructure is a blind spot in the nation's cyber defense. In order to understand and prevent threats, the government must be able to analyze attacks before, during, and after they happen. Public-private cooperation is a critical component to developing a coherent cyber defense.[10] The U.S. government cannot force private companies to disclose information on attacks to cyber systems. Yet, in order to achieve the requisite level of responsiveness, the government must be informed about current and future threats. The government must be able to identify threats and trends with enough time to respond. Requiring companies to grant government access would infringe upon civil liberties. If it facilitates an environment of information sharing, private companies can simply decline to participate. Striking the balance between civil liberties and public safety has created gridlock in Congress over how to cover this blind spot in cyber defense.

Administrative agency officials have grown impatient with the lack of cyber defense legislation. As a result, they have begun engaging the public directly about the need for a national cyber security strategy.[11] Administrative agencies are also implementing their own patchwork solutions to curb the impact of

---

[6] David Goldman, *Hacker Hits on U.S. Power and Nuclear Targets Spiked in 2012*, CNN MONEY (January 9, 2013, 1:41 PM), http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks.

[7] GMC v. Tracy, 519 U.S. 278, 289-90 (1997) (stating that regulated monopolies are consistent with the commerce clause), s*ee also* Panhandle Eastern Pipe Line Co. v. Michigan Pub. Serv. Comm'n, 341 U.S. 329, 333 (stating that public utilities sold to local private and industrial customers is generally regulated by states).

[8] GMC, 519 U.S. at 289-90.

[9] 28 U.S.C. §1346(b)(1), *see also* Richards v. United States, 369 U.S. 1, 10, (1962) (stating that the choice of law rules in state where negligence occurred apply to claims for damages).

[10] Michael Bruno, *Pentagon Nears Completion Of New Cyber Rules Of Engagement*, AEROSPACE DAILY & DEF. REPORT, Jun. 28, 2013, at 6.

[11] Leon Panetta, Sec'y, Dep't of Def., Remarks at the Bus. Execs. for Nat'l Sec. (Oct. 11, 2012), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

cyber threats. The Department of Homeland Security (the "DHS"), in particular, has implemented several innovative programs.[12] To address future threats, DHS has initiated a cyber warrior recruiting campaign on college campuses.[13] To address current threats, it has initiated programs based on public-private information sharing.[14] Although these agency programs are addressing the cyber threat and reducing the impact of cyber attacks, more must be done.

Administrative agencies should require all utility companies with government contracts to maintain a minimum level of cyber security. Cyber security requirements could seamlessly be incorporated into this well-worn framework. A minimum cyber security requirement would allow the current utilities scheme to remain intact. Contracting could be used to leverage the unique public-private relationship to its advantage. The federal government currently requires utilities to adhere to security and safety standards.[15] Specific cyber security requirements can be monitored much like physical security requirements. This minimum requirement would also reduce the government's need for information on attacks, allowing it to focus on significant threats and trends. A minimum level of cyber security in utilities would mitigate coordinated cyber attacks. The result would yield a minimum cyber defense for the most vulnerable critical infrastructure sector.

The consequences for failing to prepare for cyber warfare are a dire. The Russian invasion of Georgia is one example of how cyber attacks will likely be employed in the near future.[16] There, coordinated cyber attacks debilitated the Georgian government's communication and response nodes.[17] After Georgian cyber systems were degraded, Russia physically invaded with its military.[18] Coordinated cyber attacks of the future will certainly be larger in scope and magnitude. The cyber attacks that preceded the Georgian invasion are a clarion call for what may come if America fails to mends the holes in its cyber defense.

Part II of this note details the current utilities critical infrastructure. Part III discusses the challenges Congress faces in establishing a comprehensive cyber

---

[12] *See* US-CERT, http://www.us-cert.gov/about-us.

[13] Nicole Perloth, *Luring Young Web Warriors Is a U.S. Priority. It's Also a Game*, N.Y. TIMES, Mar. 24, 2013, http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html.

[14] *See* ICS-CERT, http://www.us-cert.gov (last visited Aug. 1, 2013).

[15] *See* FAR 52.241-6 (1995), *available at* https://www.acquisition.gov/far/reissue/FARvol2ForPaperOnly.pdf.

[16] Anne Barnard, *Georgia and Russia Nearing All-Out War*, N.Y. TIMES, Aug. 9, 2008, http://www.nytimes.com/2008/08/10/world/europe/10georgia.html.

[17] Jaak Aviksoo, Minister of Def. of the Republic of Estonia, Address at the Center for Strategic and International Studies: Cyberspace a New Dimension at our Fingertips (Nov. 28, 2007), *available at* http://csis.org/files/media/csis/events/071128_estonia.pdf.

[18] *Id.*

defense. Part IV explores patchwork solutions that administrative agencies have implemented in an effort to mitigate cyber attacks in utilities. Part V discusses how administrative agencies can leverage the existing government-contract framework to establish minimum cyber security requirements for utilities companies. Part VI illustrates the consequences for failing to establish a coherent cyber defense, using the Russian attack on Georgia as a case study.

## II. UTILITIES CRITICAL INFRASTRUCTURE

### *A. Increased Attacks*

The nation's critical infrastructure is vulnerable to cyber attack and must be protected. In recent years, critical infrastructure has increased productivity and efficiency by relying on cyberspace network control systems.[19] Critical infrastructures are the systems, networks, and assets so vital to the nation that their incapacitation or destruction would severely degrade the country's ability to function.[20] Critical infrastructures are primarily the financial, energy[21], and emergency services sectors.[22] Critical infrastructures rely on control nodes to leverage cyberspace to increase productivity and efficiency. Cyberspace is comprised of hundreds of thousands of computers, servers, and control nodes connected by fiber optic cables.[23] Cyber attacks have dramatically increased over the past decade.[24] Attacker capacity is a legitimate threat to national security. Individual groups as well as other countries are attacking utilities control nodes.[25] Those entities are bypassing the U.S.'s traditional land, sea, and air defenses by exploiting cyber vulnerabilities.[26] Utilities critical infrastructure will continue to be attacked until cyber security improves.

### *B. Market Insulation*

Utilities are insulated from the socioeconomic pressures that affect businesses in other sectors. The financial critical infrastructure sector for example, is highly sensitive to socioeconomic pressures. Cyber attacks on the financial sector erode consumer confidence, halt markets, and expose

---

[19] Napolitano, *supra* note 2.
[20] Critical Infrastructure Protections Act of 2001, §1016 42 U.S.C. §5195c (2001).
[21] In this note the energy sector is referred to as the utilities sector.
[22] 42 U.S.C. §5195c.
[23] US-CERT, THE NAT'L STRATEGY TO SECURE CYBERSPACE 1, *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.
[24] *Id*. at 6.
[25] Siobhan Gorman, *Alert on Hacker Power Play: U.S. Official Signals Growing Concern Over Anonymous Group's Capabilities*, WALL ST. JOURNAL, Feb. 21, 2012, http://online.wsj.com/article/SB10001424052970204059804577229390105521090.html.
[26] Tzu, *supra* note 1, at 62.

confidential consumer information.[27] When consumers discover that banks have lost control of their information or assets, they demand better protections. If additional protections are not provided, consumers take their business elsewhere. Socioeconomic pressures incentivize the financial sector to proactively respond to cyber related threats. Utilities are not as responsive to market pressures in part because of their legal history.

Historically, courts have validated government-subsidized monopolies in the utilities sector.[28] Courts generally have held that these monopoly arrangements are legitimate government pursuits and in accord with the Commerce Clause.[29] Unlike in the financial sector, changing regional utility providers can be a bit more challenging, if not impossible. In addition, utility companies are at times not held liable for damages caused from their services.[30] While the government may be liable for damages caused by negligence[31], state law governs whether there are grounds to bring the claim.[32] Utilities claims are filed pursuant to the choice of law rules where the alleged act occurred.[33] This legal framework provides little incentive for filing claims for damages against utilities. With limited exposure to legal recourse from consumers for damages, utilities are inadequately incentivized to increase cyber security. As a result, utilities are exposed to the threat of cyber attacks without an adequate defense.

Although helpful, self-preservation prompted by socioeconomic pressures is not the solution. The free market approach yields an unreliable patchwork defense. For example, in 2010, hackers launched a denial-of-service attack ("DoS attack") on the NASDAQ website creating a temporarily jolting disruption

---

[27] Jenny B. Davis, *Cybercrime Fighters: Companies Have More Legal Weapons to Defend Against Attacks on Their Computer Systems*, 89 A.B.A. J., Aug. 2003, at 36.

[28] GMC, 519 U.S. at 289-90. (1997), *see also* Panhandle Eastern Pipe Line Co., 341 U.S. at 333.

[29] Huron Portland Cement Co. v. Detroit, 362 U.S. 440, 443-44 (1960) (stating that state actions that indirectly affect commerce do not prohibit states from legislating on the health, life, and safety of their citizens, though the legislation might indirectly affect commerce), *see also* Gibbons v. Ogden, 22 U.S. at 1, 21 (1824) (stating that States can enact legislation that creates monopolies and regulate commerce for the advantage of the community so long as it does not encroach on ground constitutionally reserved for the exclusive control of Congress.), *see, e.g.,* Hall v. De Cuir, 95 U.S. 485, 488 (1878) (stating that state legislation that regulates commerce within the state but does not seek to influence interstate commerce does not violate interstate commerce).

[30] Maxim Integrated Prods. v. United States*,* 1988 Cal. Unrep., *1, *18 (N.D. Cal. Dec. 4, 1998).

[31] 28 U.S.C. § 1346(b)(1), s*ee also* United States v. Muniz, 374 U.S. 150, 153 (1963) (stating that a claim against the government can be made where a private person under like circumstances would be liable under state law).

[32] United Scottish Ins. Co. v. United States., 614 F.2d 188, 195-96 (9th Cir. 1979).

[33] 28 U.S.C. §1346(b)(1); *see also* Richards, 369 U.S. at 10.

of the market.[34] DoS attacks seek to make cyber systems inaccessible by engaging them for prolonged periods of time from thousands of individual computers.[35] In 2011, the hacker group "Anonymous" attempted to "erase" the NYSE webpage as a gesture of support for the Occupy Wall Street protests.[36] These examples illustrate the limitations of relying solely on socioeconomic pressures as a defense to cyber attacks. Yet, as thin as the layer of cyber security in the financial sector is, it is virtually non-existent in the utilities sector.

### *C. Calls for Action*

The chorus of U.S. officials warning about utilities vulnerabilities is growing. Within the various echelons of the U.S. government, agency leaders are voicing their concerns about cyber attacks. Former Secretary of Defense Leon E. Panetta compared the current cyber threat to Pearl Harbor.[37] The Secretary's World War II analogy warns of a large-scale surprise attack on several critical infrastructures. The result of that attack would be a massive disruption of services and loss of life.[38] According to Panetta, hackers have already infiltrated electricity and water plant cyber control systems.[39] Echoing Panetta, Secretary of State John Kerry, during his Senate confirmation hearings, warned the Senate Foreign Relations Committee of the dangers cyber attacks pose to the nation's energy sector.[40] Secretary of the Department of Homeland Security Janet Napolitano characterized utilities attacks as setting up a potential "cyber 9/11."[41] In the absence of legislative solutions, these agency heads are implementing stopgap measures to combat cyber threats.

---

[34] Michael J. McFarlin, *NASDAQ, CBOE, Bats Hit by Cyber-Attacks*, THE FUTURES MAGAZINE, Feb. 15, 2012, http://www.futuresmag.com/News/2012/2/Pages/Bats-CBOE-Nasdaq-hit-by-cyberattack.aspx.

[35] John Markoff, *Georgia Takes a Beating in the Cyberwar With Russia*, N.Y. TIMES, Aug. 11, 2008, http://bits.blogs.nytimes.com/2008/08/11/georgia-takes-a-beating-in-the-cyberwar-with-russia/.

[36] *Id.*

[37] Panetta, *supra* note 9.

[38] Elizabeth Bumiller, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES, Oct. 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

[39] *Id*.

[40] Gerry Smith, *John Kerry: Foreign Hackers Are '21st Century Nuclear Weapons'*, HUFFINGTON POST, Jan. 24, 2013, http://www.huffingtonpost.com/2013/01/24/john-kerry-hackers_n_2544534.html.

[41] Jim Finkle, *Cyber 9/11 could happen 'imminently,' says US Homeland Security chief*, REUTERS, Jan. 24, 2013, http://www.nbcnews.com/technology/technolog/cyber-9-11-could-happen-imminently-says-us-homeland-security-1C8103556.

## III. The Role of Congress in Finding a Solution

### A. *Cyber Security Legislation*

Congress must find a way to pass comprehensive cyber security legislation. Congress is the only governmental body capable of creating a comprehensive cyber security plan.[42] Cyber security legislation has steadily gained support for securing critical infrastructure since the year 2000.[43]

One of the most comprehensive cyber-security bills was the Cyber Security Enhancement Act of 2012 ("CSA2012").[44] The bill never made it out of committee however, failing to acquire the 60 votes needed for a Senate general member vote.[45] CSA2012 attempted to tackle two of Congress' biggest challenges: (1) maintaining civil liberties, and (2) ensuring public safety. The bill addressed civil liberties in Section 204 through the promotion of public awareness and education about current cyber threats.[46] The section called for efforts to make cyber security best practices known and usable to all public businesses.[47] The effort was strengthened by a late amendment that specifically allowed the government to share threat information with private industries controlling critical infrastructure.[48] These were much-needed steps in the right direction.

### *B. Providing for Security*

The public must be informed of the threats cyber attacks pose to national security. Section 203 of the bill addressed the security technical standards for providing adequate security to critical infrastructure.[49] Specifically, Section 203 called for the accelerated development of interoperable security standards to secure interoperability between the government and private businesses.[50] The section also called for security frameworks that complied with privacy

---

[42] Napolitano, *supra* note 2.
[43] Cyber Security Information Act of 2000, H.R. 4246, 106th Cong., §§2-6 (2000).
[44] Cybersecurity Enhancement Act of 2012, H.R.2096, 112th Cong., §§101-06 (2011).
[45] Michael Schmidt, *Cybersecurity Bill Is Blocked in Senate by G.O.P. Filibuster*, N.Y. Times, Aug. 2, 2012, http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html.
[46] H.R. 2096, 112th Cong. (2012).
[47] *Id*.
[48] Cyber Intelligence Sharing and Protection Act of 2012, *amended by* H.R. 3523, 113th Cong. (2012) (amending CISPA to make explicit that nothing in the legislation would prohibit a department or agency of the federal government from providing cyber threat information to owners and operators of critical infrastructure).
[49] *Id*.
[50] *Id*.

requirements.[51] This was an effort to ensure a firm line between public and private cooperation would be observed. Interoperability, collaboration, and privacy assurance are essential to creating a coherent cyber defense network that spans government and private business systems.

*C. Cyber Security Legislation in 2013*

The Cyber Security and American Cyber Competitiveness Act of 2013 ("S.21") was introduced to the Senate and referred to the Committee on Homeland Security and Government Affairs.[52] S.21 sets a broad set of criteria in order to gain consensus. Specifically, it seeks to create a framework for developing public-private systems that protect critical infrastructure, such as utilities.[53] A focal point of S.21 is the attempt to find the balance been civil liberties and public safety that CSA2012 could not.[54] Although the bill is in its initial stages, Congress should incorporate the sections 203 and 204 of CSA2012. Those sections should be foundational components of the legislation because they contain innovative proposals for public safety and the protection of civil liberties.

*D. The Fourth Amendment*

The legislative solution must be congruent with the spirit and the letter of the Fourth Amendment of the U.S. Constitution. The Fourth Amendment affords U.S. citizens the right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.[55] In order to prevent warrantless monitoring, the Fourth Amendment must govern any proposal for government access to private utilities networks.[56] Yet, some government officials have proposed unilateral executive action. Notably, Secretary Panetta stated that, although there is no substitute for legislation, the Obama administration is working on an executive order on cyber security.[57] Although Panetta's appeals to urgency may be well founded, government intrusion into private businesses is not a solution.

---

[51] *Id*.
[52] LIBRARY OF CONG., BILL SUMMARY AND STATUS H.R. 3523, 113TH CONG. (May 7, 2012), http://thomas.loc.gov/.
[53] *Id*.
[54] *Id*.
[55] U.S. CONST. amend. IV.
[56] Lolita Baldor, *U.S. Cybersecurity Efforts Trigger Privacy Concerns*, WASH. TIMES, Jan. 27, 2012, http://www.washingtontimes.com/news/2012/jan/27/cybersecurity-efforts-trigger-privacy-concerns.
[57] Nicholas Hoover, *DOD: Hackers Breached U.S. Critical Infrastructure Control Systems*, INFO. WEEK, Oct. 12, 2012, http://www.informationweek.com/government/security/dod-hackers-breached-us-critical-infrast/240008972.

The U.S. government cannot handle this threat alone. Government intrusions into homes and businesses will not create secure cyber networks. The interdependent relationship between government and critical infrastructure companies relies on each party accessing cyberspace to secure the space that they own, or operate in.[58] Director of the National Security Agency General Keith Alexander noted that complex problems posed by cyber attacks do not require sacrificing civil liberties for security.[59] Establishing a common ground between security and civil liberties should be a starting point in establishing a comprehensive cyber defense.

*E. Learning from Past Failures*

The role of technology in the debate between civil liberties and public safety is not new. In the 1928 case *Olmstead v. United States*, the Supreme Court debated whether the advantages gained over certain criminal activity warranted narrowing the Fourth Amendment of all citizens.[60] There, the Court held that the use of evidence from private telephone conversations intercepted by wire-tapping was not a violation of the Fourth Amendment because the threat outweighed the need for civil liberties.[61] There, the Supreme Court prescribed an unimaginatively rigid solution that resulted in legal government wiretapping. The United States cannot afford repeat the mistakes made in cases like *Olmstead*. As in Sections 203 and 204 of CSA2012, the government must promote solutions that conform to the Fourth Amendment while ensuring adequate cyber security.[62] Handwringing is not a plan. Although vigilance is tempered by the knowledge that the greatest threats to freedom come in times of crisis,[63] the U.S. government cannot give in to the stagnating principle of paralysis by analysis.

---

[58] THE NAT'L STRATEGY TO SECURE CYBERSPACE, *supra* note 21, at 11.

[59] James Ryan, *NSA Director on Cyberattacks: 'Everybody's Getting Hit'*, ABC NEWS, Nov. 7, 2012, http://abcnews.go.com/blogs/politics/2012/11/nsa-director-on-cyberattacks-everybodys-getting-hit/.

[60] Olmstead v. United States, 227 U.S. 438 (1928) *overruled by* Katz v. United States, 389 U.S. 347 (1967) (holding that Court's immaterial intrusions using technology as a search can constitute an unreasonable search and seizure pursuant to the Fourth Amendment and expanded its reach to provide protection to all areas a person has a reasonable expectation of privacy).

[61] *Id.*

[62] *See* H.R. 2096, 112th Cong. (2011).

[63] Vernonia School Dist. 47J v. Action, 515 U.S. 646 (1995) (Justice O'Connor dissenting, stating that student athletes' expectation of privacy outweighs public hysteria and demands for public safety).

*F. Public-Private Partnership is Essential*

The government must work with, rather than act upon privately owned utilities. There is an interdependent relationship between utilities critical infrastructures and the private companies that own and operate them.[64] The balance in the public-private relationship would be shattered if an *Olmstead* approach prevailed. Government officials that push for coercive measures should be mindful not to alienate private businesses. Congress must continue to work on creating a solution that fosters public-private cooperation. The government must strive to work with private utility companies on common grounds. The largest of which is the protection of private assets that directly impact the lives of many citizens.

The government seems to understand its burden in creating an amicable environment for information sharing. The government's approach to the Einstein 3 program is an example of how it can inform and build public confidence in cyber security. Einstein 3 is a government network monitoring system that detects and reacts to cyber attacks on federal systems.[65] DHS officials have encouraged an open dialogue about the program in an effort to illustrate the extensive privacy protections already in place.[66] Such is a much needed gesture on behalf of the government to build public "trust and strict confidentiality" in the program.[67] An environment where the government and private companies freely exchange cyber threat information is a superior model to that of government monitoring. The goal of information sharing should be to create a seamlessly integrated cyber defense that blocks or blunts attacks. As cyber attacks continue to grow in intensity and frequency, the consequences of failure become more severe.

*G. Avoiding Reactionary Measures*

Congress has an opportunity to balance security and civil liberties while the threat is still manageable. Other countries have avoided the issue and are now taking drastic measures to address cyber threats. Australia and Great Britain, for example, are forcing private companies to invest resources in cyber defense and share internal data about attacks.[68] In Great Britain, cyber attacks are now regarded as a top threat to national security.[69] Those drastic measures were

[64] THE NAT'L STRATEGY TO SECURE CYBERSPACE, *supra* note 21, at 2.
[65] Baldor, *supra* note 50.
[66] *Id.*
[67] *Id.*
[68] Gillian Tett, *Time to Break Wall of Silence on Escalating Cyber Attacks*, FIN. TIMES, Jan. 25, 2013, https://www.fidelity.co.uk/investor/news-insights/expert-opinions/details.page?whereParameter=gillian-tett/escalating-cyber-attacks.
[69] Francis Maude, Member of British Parliament, Address at the International Center for

taken because the privately owned critical infrastructure sectors failed to maintain inadequate cyber security.[70] Congress can avoid resorting to draconian measures by promoting information sharing and establishing minimum cyber security standards in legislation.[71] Congress can only pass legislation by working on common ground to shore up the weak links in the cyber defense chain.

## IV. PATCHWORK SOLUTIONS

### *A. Administrative Agency* Solutions

In the wake of persistent attacks, administrative agencies are creating patchwork cyber solutions. Administrative agencies are semi-autonomous government bodies that execute legislative, judicial, or executive functions.[72] The apolitical nature of administrative agencies enables them to create solutions to large problems while withstanding political pressure.[73] One agency that has been particularly active in establishing cyber security measures is the Department of Homeland Security. Congress established DHS as one of the fifteen administrative agencies of the executive branch.[74] It is responsible for preventing and minimizing terrorist attacks on the U.S.[75] The Department's attempts to tackle cyber security problems provide examples of how administrative agencies can provide intermediate solutions to politically complex problems.

### *B. The Department of Homeland Security*

#### i. Recruiting Future Cyber Warriors

DHS has established several programs to combat cyber threats. One program focuses on recruiting future cyber security specialists on college campuses. At San Jose State University, for example, Secretary Napolitano laid out a plan to build a cyber security workforce to combat cyber attacks in an address to students.[76] At George Mason University, DHS created a cyber

---

Defense Studies in Estonia (May 3, 2012), *available at* https://www.gov.uk/government/speeches/francis-maude-speech-at-the-international-centre-for-defence-studies-icds-in-Estonia.

[70] *Id.*

[71] Napolitano, *supra* note 2.

[72] Peter L. Strauss, *The Place of Agencies in the Government: Separation of Powers and the Fourth Branch of Government*, 84 COLUM. L. REV. 573, 583-84 (1984) (identifying modern functions of administrative agencies).

[73] *Id.* at 586.

[74] Executive Departments, 5 U.S.C. § 101 (2013).

[75] Homeland Security Act of 2002, P.L. 107-296, 107th Cong. (2002).

[76] Napolitano, *supra* note 2.

specialist recruiting competition called the "Virginia Governor's Cup Cyber Challenge."[77] The competition was modeled on a program implemented by the Chinese government.[78] The government must continue these recruiting programs to prepare for future threats. In addition to preparing for future threats, DHS established programs to deal with current threats.

ii. Addressing Current Threats to Utilities

DHS programs rely on overt government monitoring and self-reporting. The U.S. Computer Emergency Readiness Team ("US-CERT") is a watch and warning center that responds to cyber security threats to infrastructure systems.[79] It is a system that detects attacks after they have occurred. The focus of US-CERT is rapid response and damage mitigation. The program enables the government to repair infrastructure cyber systems soon after they are detected. In its current application, US-CERT is a completely reactionary program. Conversely, the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") attempts to reduce threats to utilities based on self-reporting.[80] It partners intelligence and law enforcement agencies with private utilities to collaborate and share cyber threat information.[81] The program provides private utilities an opportunity to interface with government agencies about the vulnerabilities of their cyber control nodes before a debilitating attack.[82] This forward-thinking program captures the tone the legislature should seek to replicate in legislation.

ICS-CERT fosters the public-private relationship between utilities and government agencies. It also functions as an on-call incident response team that provides situational awareness and triages cyber attacks on critical infrastructure.[83] In 2010, the first full year of ICS-CERT, DHS recorded 41 reported attacks on utilities.[84] In the year 2011 the number rose to 198.[85] All reported attacks were conducted through cyberspace using methods ranging from spear phishing to website hyperlinks.[86] The main drawback to this

---

[77] Nicole Perloth, *Luring Young Web Warriors Is a U.S. Priority. It's Also a Game*, N.Y. TIMES, Mar. 24, 2013, http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html.
[78] *Id*.
[79] US-CERT, *supra* note 9.
[80] Critical Infrastructure Sec. and Resilience, Presidential Policy Directive 21 (2013).
[81] *Id.*
[82] ICS-CERT, *supra* note 11.
[83] U.S. DEP'T OF HOMELAND SECURITY, ICS-CERT INCIDENT RESPONSE SUMMARY REPORT 2009-2011 17, http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29.pdf.
[84] *Id.* at 5.
[85] *Id*.
[86] *Id.* at 13.

program, however, is that it relies on volunteer reporting from companies that have little incentive to participate. This self-reporting method, although helpful, is only a fraction of what is required to combat cyber threats.

iii. Severity of the Threat

Unreported cyber threats can lead to debilitating consequences. In August 2003, an unreported Internet computer worm corrupted the control systems of Ohio's Davis-Besse Nuclear Power Plant.[87] The attack left thousands without power four hours. Similarly, an attack on utility control systems that manage dams could cause an overflow, which would devastate a local area.[88] A coordinated attack on multiple power plants would result in massive catastrophe and would lead to the displacement of countless Americans.[89] Of additional concern is the fact that the federal government and the Department of Defense purchase over 29 million megawatt-hours of electricity annually.[90] A well-coordinated attack on utilities could significantly impact the government's ability to function.

Utilities are the most targeted of all critical infrastructure sectors. While the exact number of attacks on utilities is unknown, it is clear that attacks are increasing. Approximately 60% of all cyber attacks on critical infrastructures in the year 2011 were on utilities.[91] In the year 2012, ICS-CERT estimated approximately 7,2000 utility control system devices were targeted by advanced persistent threat activity.[92] Analysis of these trends highlights both the gaunt state of the U.S.'s utility cyber security and the opportunistic nature of cyber attackers. It is sobering to note that those reports only reflect reported attacks. Despite the efforts of DHS to work with private businesses, there is no way to tell how many cyber attacks go unreported. The U.S.'s critical infrastructure should not depend on private companies volunteering information. Congress must enact comprehensive legislation that provides a baseline cyber security defense.

---

[87] Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant Network*, SEC. FOCUS, Aug. 19, 2003, http://www.securityfocus.com/news/6767.

[88] Natasha Solce, *The Battlefield Of Cyberspace: The Inevitable New Military Branch - The Cyber Force*, 18 Alb. L.J. Sci. & Tech. 293, 303 (2008).

[89] Napolitano, *supra* note 2.

[90] Anthony Andrews, *Federal Agency Authority to Contract for Electric Power and Renewable Energy Supply Study*, CONG. RESEARCH SERV. 1 (Aug. 15, 2011), http://www.nationalaglawcenter.org/assets/crs/R41960.pdf.

[91] ICS-CERT, *supra* note 75, at 5.

[92] U.S. DEP'T OF HOMELAND SECURITY, ICS-CERT MONITOR OCT./NOV./DEC. 2012 4-5, *available at* http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf.

## V. CONTRACTING A STOPGAP FROM THE EXISTING UTILITIES FRAMEWORK

### *A. How Contracting Can be Effective*

Administrative agency contracting would provide a stopgap solution to the utilities cyber security problem. The government has the authority to enter into contracts with private utilities.[93] Contracting would affect utilities in a way that market pressures do not. Government contracting could nudge the utilities sector to change, update, or modernize their cyber security systems in order to stay in business. Through contracting, the federal agencies could require private utility companies to comply with minimum cyber security standards. Minimum standards could be used as the entry criteria for bidding and maintaining government contracts. This would increase the amount of utilities implementing adequate cyber security while creating a uniform line of defense.

### *B. Using Preexisting Contract Frameworks*

Although there is currently no minimum cyber security requirement for utilities contracts, the framework for physical security is well established. The government has the authority to regulate privately owned utilities in the interest of public safety.[94] Several examples include the Public Utilities Holding Company Act ("PUHCA"), the Federal Property Administration Act ("FPAA"), and Title 42 of the United States Code. PUHCA requires companies to report specific information to the government on the grounds of public safety.[95] FPAA is a Department of Energy ("DOE") regulation, which grants the General Services Administration the authority to establish methods and policies for acquiring utility services to federal agencies.[96] FPAA may be able to add cyber policy requirements at its discretion. Title 42 of the United States Code authorizes the DOE to initiate and modify energy contracts with private utilities companies.[97] Accordingly, the DOE may be able to incorporate cyber requirements into contracts as well.

---

[93] Department of Energy Acquisition Policy, 48 C.F.R. §41.103 (2013); *See also* Anthony, *supra* note 80, at 3.

[94] *See PG&E Corp. v. Public Utilities Com.*, 118 Cal. App. 4th 1174, 1184 (Cal. App. 1st Dist. 2004) (establishing that the Commission has the authority to impose and enforce actions pursuant to enforcement of the Public Utilities Act)*; see also General Tel. Co. v. Public Utility Com.,* 628 S.W.2d 832, 839 (Tex. App. Austin 1982).

[95] *See* Joseph Woodle, Dir. Div. of Corp. Regulation SEC., Remarks at Conference on Securities Laws and Regulation (Feb. 19-20, 1959), http://www.sec.gov/news/speech/1959/0219-2059woodle.pdf; *see also PG&E Corp*., Cal. App. 4th at 1184; *see also General Tel. Co*., 638 S.W. 2d at 839.

[96] Fed. Prop. and Admin. Serv. Act of 1949, 40 U.S.C. § 201 (2000).

[97] 42 U.S.C. §7256 (2006).

i. Two Potential Approaches

Between PUCHA and FPAA two potential contractual approaches emerge. In the first approach utilities would agree to government monitoring. The government would monitor internal business networks to ensure minimum cyber security requirements are maintained. Enacted in 1935, PUCHA was implemented to protect consumers from risky utility company practices.[98] It is one example of how administrative agencies could use contracts to increase cyber security by monitoring. In 2005, the reformed PUHCA maintained its oversight requirement to ensure utilities remain reliable and functional.[99] Additionally, the Act requires utilities holding companies to make their financial books, accounts, memoranda, and costs available for government review.[100] Accordingly, this framework may allow administrative agencies to requirement utilities to report expenses spent preventing or rebuilding after network attacks. Similarly to the present situation, at that time utilities companies leveraged the short-term benefits of risky behavior while exposing the population to unacceptable risks.[101] This utilities-focused regulation is an example for how administrative agencies can enhance cyber security through contracting.

PUHCA has the internal mechanics required to regulate and enforce cyber security through contracting. Specifically, Section 366.1 establishes the Federal Energy Regulation Commission ("FERC") as the administrative action for enforcing PUCHA.[102] FERC is an independent agency that regulates the interstate transmission of utilities.[103] FERC enforces regulatory requirements through the imposition of civil penalties and punishments.[104] Its mission is to promote the development of safe, reliable, and efficient utilities infrastructure that serves the public interest.[105] The purpose for requiring government access to sensitive information was for the protection of the populace. As a safeguard for preventing a company's sensitive internal information, Section 1264(d)

[98] *See* Remarks from Joseph Woodle, *supra* note 87, at 1.

[99] FED. ENERGY REGULATION COMM'N, FEDERAL ENERGY REGULATION FACT SHEET ENERGY POLICY ACT 2005 (2006), *available at* http://www.ferc.gov/legal/fed-sta/epact-fact-sheet.pdf.

[100] Energy Policy Act of 2005, Pub. L. No. 109–58, § 1275(b) 119 Stat. 594, 977 (2005); *see also* Morgan Stanley Capital Grp., Inc. v. Pub. Util. Dist. No. 1 of Snohomish Cnty., 554 U.S. 527, 531, (2008) (holding that energy companies must file their rate schedules and service contracts).

[101] *See* Remarks from Joseph Woodle, *supra* note 87, at 1.

[102] Repeal of the Public Utility Holding Company Act of 1935 and Enactment of the Public Utility Holding Company Act of 2005, 18 C.F.R. § 335 (2005) (repealed 2005), *available at* http://www.ferc.gov/whats-new/comm-meet/091505/M-1.pdf.

[103] FERC, WHAT FERC DOES, http://www.ferc.gov/about/ferc-does.asp (last visited Aug. 1, 2013).

[104] *Id*.

[105] U.S. FED. ENERGY REGULATION COMM'N, THE STRATEGIC PLAN, FISCAL YEAR 2009-2014 3 (Revised 2013), *available at* https://www.ferc.gov/about/strat-docs/FY-09-14-strat-plan-print.pdf.

forbid any one with access to this information from disclosing it.

Required reporting and internal systems monitoring would aid established programs like ICS-CERT, but at too high a cost. The government would gain the benefit of not having to rely on volunteer information. Mandatory reporting may even increase government efficiency in preventing future attacks. One glaring drawback to this approach, however, is that it would put the solution squarely in the same position that Congress now finds itself in. This approach would all but certainly aggravate the ongoing civil liberties—public safety debate in Congress. Such an approach would likely frustrate the public-private relationship and create more problems than it would solve. A contract policy requiring private companies to allow government monitoring of internal cyber systems would likewise be doomed to failure.

In the second approach, administrative agencies merely verify that minimum cyber security standards are in place. This approach would consist of government verification of cyber security standards. DOE Federal Acquisition Regulation ("FAR") requires all federal agency utilities contracts comply with its service provisions.[106] This less intrusive framework allows utilities to meet standards set and verified by the government through inspections.

FAR has the requisite structure to enforce a cyber capabilities inspection program. FAR, Section 52.241-6, specifies the physical requirements utilities must maintain to be in compliance with the contract.[107] While this area focuses on physical equipment, it could be expanded to address cyber security. This section calls for government participation in facility inspections to ensure utilities remain in compliance with the terms of the contract. This approach calls for reviewing utilities cyber security without invasive monitoring. Administrative agency inspections could have a significant impact on utilities.

This approach would give private utilities the freedom to choose how to meet the government's standards. It would also avoid the ongoing civil liberties debate that has gridlocked Congress.

## VI. CONSEQUENCES OF FAILING TO ACT

### A. *Attacks in Perspective*

The consequences of failing to act would be disastrous. US-CERT has already responded to more than 106,000 incident reports of cyber attack to the critical infrastructure since the program began.[108] When viewed in a vacuum, one may be tempted to dismiss the national concern. Yet, when viewed as a trend, the

---

[106] FAR 52.241-6 (1995), *available at* https://www.acquisition.gov/far/reissue/FARvol2ForPaperOnly.pdf.
[107] *Id*.
[108] Napolitano, *supra* note 2.

national significance arises to the foreground.

B. *Cyber Attack on Georgia*

The cyber attack on the country of Georgia illustrates how cyber warfare will be used in future conflicts. In August 2008, Georgian forces launched an attack against separatist forces sympathetic to Russia.[109] Shortly thereafter, the Russian military invaded Georgia.[110] Before the Russian invasion, Georgia's governmental cyber systems were attacked.[111] The attack was broad and coordinated. The volume of Internet traffic into Georgia increased by 400 times during the attack.[112] The DoS attack disrupted the Georgian government's ability to function and respond to the Russian invasion. The cyber attacks on Georgia began weeks before it was physically invaded.[113] This was the first time a cyber attack immediately preceded a physical attack between two sovereign nations.[114] It will likely not be the last.

C. *Cyber Attacks in the Future*

A fundamental tenet of warfare is deception.[115] The ability to leverage cyber attacks while remaining unidentified is a bellwether for future warfare.[116] Cyber attacks are relatively inexpensive, easy to execute, and the perpetrators rarely get caught.[117] As technology like the kind used in Georgia becomes more available, entities will continue to exploit cyber weaknesses in nations' critical infrastructures.[118] To this day the attacks on Georgia's cyber systems are

---

[109] *See* Anne Barnard, *Georgia and Russia Nearing All-Out War*, N.Y. TIMES, Aug. 9, 2008, http://www.nytimes.com/2008/08/10/world/europe/10georgia.html.

[110] *Senior Georgian Ministers Sacked,* BBC NEWS, (Dec. 5, 2008), http://news.bbc.co.uk/2/hi/europe/7767799.stm.

[111] *CNN American Morning: What Can the U.S. Do to Deal With the Russian Invasion of Georgia?* (CNN television broadcast Aug. 14, 2008, 7:47 AM) *available at* https://advance.lexis.com/.

[112] Jaak Aviksoo, Minister of Def. of the Republic of Estonia, Address at the Center for Strategic and International Studies: Cyberspace a New Dimension at our Fingertips (Nov. 28, 2007), *available at* http://csis.org/files/media/csis/events/071128_estonia.pdf.

[113] *The cyber raiders hitting Estonia*, BBC NEWS (May 17, 2007, 14:52 GMT), http://news.bbc.co.uk/2/hi/europe/6665195.stm.

[114] See Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAGAZINE, Aug. 21, 2007, *available at* http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

[115] Tzu, *supra* note 1, at 42.

[116] William C. Ashmore, *Impact of Alleged Russian Cyber Attacks Impact of Alleged Russian Cyber Attacks*, SCHOOL OF ADVANCED MILITARY STUDIES, 12 (2008), *available at* http://www.dtic.mil/dtic/tr/fulltext/u2/a504991.pdf.

[117] John Markoff, *Before Gunfire, Cyber Attacks*, N.Y. TIMES, Aug. 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[118] Robert Gates, Sec'y of Def., Keynote Address at the Army War College (Apr. 16, 2009); *see*

unattributed.[119] With the successful attacks on Georgia firmly in mind, it is imperative that America solve its' cyber security issues.

## VII. CONCLUSION

America's critical infrastructure is vulnerable to cyber attacks. Threats and attacks to the U.S.'s utilities sector are not hypothetical—they are real and ongoing. The utilities sector is the most vulnerable critical infrastructure sector. They have come to rely on cyber controls to cut costs and increase efficiency. They have not however, reciprocally increased their cyber-security posture. Utilities have become the target of choice for cyber attackers. The public-private relationship between the government and utility companies has compounded the problem. Without market pressures, or the threat of suits for failures in service, utilities are lagging behind in cyber security. The stakes are too high to rely solely on individual companies to defend the nation's critical infrastructure. Only legislation passed by the U.S. Congress can provide comprehensive national defense to combat cyber threats.

Congress must find a workable solution to this complex problem. Central to the hotly contested cyber defense issue is the balance between civil liberties and public safety. The answer lies firmly in the confines of partnership between the government and private companies. Congress must foster an environment that promotes information sharing that reflects partnership. Resolving civil liberties issues has proven to be a daunting task; yet, while progress is being made cyber attacks continue to grow in frequency and magnitude.

Administrative agencies can immediately begin implementing stopgap cyber defense measures through contracting. The precedence, framework, and mechanics for utilities regulation pursuant to public safety are well established. Currently, agency contracts require specific and general physical security standards. However, they do not yet require a minimum cyber security threshold for acquiring or bidding on utility contracts. Contracting requirements allow the bidder to choose their own products and maintain their own systems. Although public-private information sharing and contracting is not a total solution, it would certainly help. Administrative agency contracting is an appropriate stopgap because it increases public safety without

---

*also* THE NAT'L STRATEGY TO SECURE CYBERSPACE, *supra* note 21, at 7; *see also* Jeanne Meserve, *Study Warns of Cyberwarfare During Military Conflicts*, CNN, Aug. 17, 2009, http://www.cnn.com/2009/US/08/17/cyber.warfare/.

[119] *See* Mark Rutherford, *Report: Russian Mob Aided Cyberattacks on* Georgia, CNET NEWS, Aug. 18, 2009, http://news.cnet.com/8301-13639_3-10312708-42.html*; see also* Mike Collier, *Estonia: Cyber Superpower*, BLOOMBERG BUSINESS WEEK, December 17, 2007, http://www.businessweek.com/stories/2007-12-17/estonia-cyber-superpowerbusinessweek-business-news-stock-market-and-financial-advice.

encroaching on civil liberties. This stopgap would give the Congress breathing room to find an appropriate solution.

The consequences for failure to act are glaring. The cyber attack that preceded the invasion of Georgia was a clarion call for all nation-states. An attack on the United States will likely not come in the form of smoldering ships in the nation's seaports, or planes crashing into buildings—it will be with the anonymous click of a mouse that turns off our power grids, releases flood waters of dams, and melts down nuclear reactors.

America must continue pressing on towards a coherent solution with the understanding that civil liberties and national defense are not mutually exclusive of one another. Yet, as this debate continues, threats to the U.S.'s infrastructure become more sophisticated and effective. Only a comprehensive solution is capable of mending the gaping holes in the nation's common cyber defense.